

LFM



PATENT  
B588-042

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s) : Satoru Wakao, Akira Akashi  
Serial No. : 10/797,827  
Filed : March 10, 2004  
For : DIGITAL SIGNATURE GENERATING APPARATUS, METHOD,  
COMPUTER PROGRAM AND COMPUTER-READABLE STORAGE  
MEDIUM  
Examiner : Unassigned  
Art Unit : 2131

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

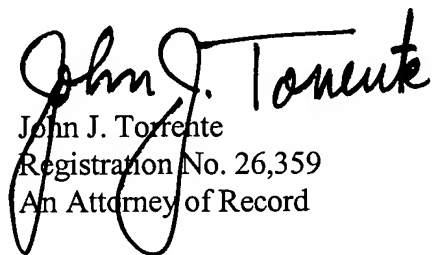
CLAIM TO BENEFIT OF 35 U.S.C. § 119  
AND FILING OF PRIORITY DOCUMENT

Claim is made herein to the benefit of 35 U.S.C. § 119 of the filing date of the  
following Japanese Patent Application: 2003-071033 (filed March 14, 2003) a certified copy of  
which are filed herewith.

Dated: August 17, 2004

Respectfully submitted,

COWAN, LIEBOWITZ & LATMAN, P.C.  
1133 Avenue of the Americas  
New York, NY 10036-6799  
(212) 790-92000

  
John J. Torrente  
Registration No. 26,359  
An Attorney of Record

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to:  
Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on:

August 17, 2004  
Date of Signature  
John J. Torrente  
Signature

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日                      2 0 0 3 年    3 月 1 4 日  
Date of Application:

出 願 番 号                      特 願 2 0 0 3 - 0 7 1 0 3 3  
Application Number:

[ST. 10/C]:                      [ J P 2 0 0 3 - 0 7 1 0 3 3 ]

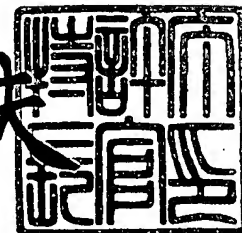
願                      人                      キヤノン株式会社  
Applicant(s):

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2 0 0 4 年    3 月 2 9 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫





【書類名】 特許願

【整理番号】 253927

【提出日】 平成15年 3月14日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00

【発明の名称】 デジタル署名生成装置、方法、コンピュータプログラム  
、およびコンピュータ読み取り可能な記憶媒体

【請求項の数】 12

【発明者】

    【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会  
社内

    【氏名】 若尾 聡

【発明者】

    【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会  
社内

    【氏名】 明石 彰

【特許出願人】

    【識別番号】 000001007

    【氏名又は名称】 キヤノン株式会社

【代理人】

    【識別番号】 100090273

    【弁理士】

    【氏名又は名称】 國分 孝悦

    【電話番号】 03-3590-8901

【手数料の表示】

    【予納台帳番号】 035493

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1



【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705348

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 デジタル署名生成装置、方法、コンピュータプログラム、およびコンピュータ読み取り可能な記憶媒体

【特許請求の範囲】

【請求項 1】 複数の秘密鍵を記憶した記憶手段とを有するデジタル署名生成装置であって、

鍵変更コマンドを受信した場合には、前記デジタル署名生成装置が使用する秘密鍵を前記鍵変更コマンドが指定する秘密鍵に変更し、

署名生成コマンドを受信した場合には、前記複数の秘密鍵の何れか一つを用いてデジタルデータのデジタル署名を生成することを特徴とするデジタル署名生成装置。

【請求項 2】 前記デジタル署名生成装置は、ICカードであることを特徴とする請求項 1 に記載のデジタル署名生成装置。

【請求項 3】 前記デジタル署名生成装置は、マルチアプリケーション OS を搭載した装置であることを特徴とする請求項 2 に記載のデジタル署名生成装置。

【請求項 4】 前記鍵変更コマンドは、前記複数の秘密鍵の何れか一つを指定する情報を含むコマンドであることを特徴とする請求項 1～3 のいずれか 1 項に記載のデジタル署名生成装置。

【請求項 5】 署名生成コマンドは、前記デジタルデータのハッシュ値を含むコマンドであることを特徴とする請求項 1～4 のいずれか 1 項に記載のデジタル署名生成装置。

【請求項 6】 複数の秘密鍵を記憶した記憶手段とを有するデジタル署名生成装置におけるデジタル署名生成方法であって、

鍵変更コマンドを受信した場合には、前記デジタル署名生成装置が使用する秘密鍵を前記鍵変更コマンドが指定する秘密鍵に変更する工程と、

署名生成コマンドを受信した場合には、前記複数の秘密鍵の何れか一つを用いてデジタルデータのデジタル署名を生成する工程とを有することを特徴とするデジタル署名生成方法。

【請求項 7】 前記デジタル署名生成装置は、ＩＣカードであることを特徴とする請求項 6 に記載のデジタル署名生成方法。

【請求項 8】 前記デジタル署名生成装置は、マルチアプリケーションＯＳを搭載した装置であることを特徴とする請求項 7 に記載のデジタル署名生成方法。

【請求項 9】 前記鍵変更コマンドは、前記複数の秘密鍵の何れか一つを指定する情報を含むコマンドであることを特徴とする請求項 6 ～ 8 のいずれか 1 項に記載のデジタル署名生成方法。

【請求項 10】 署名生成コマンドは、前記デジタルデータのハッシュ値を含むコマンドであることを特徴とする請求項 6 ～ 9 のいずれか 1 項に記載のデジタル署名生成方法。

【請求項 11】 請求項 6 ～ 10 のいずれか 1 項に記載のデジタル署名生成方法の各工程をコンピュータに実行させることを特徴とするコンピュータプログラム。

【請求項 12】 請求項 11 に記載のコンピュータプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタルデータ（画像データなど）のデジタル署名を生成するデジタル署名生成装置、方法、コンピュータプログラム、およびコンピュータ読み取り可能な記憶媒体に関するものである。

【0002】

【従来の技術】

現在、デジタルカメラなどの撮像装置で撮像されたオリジナル画像データのデジタル署名をＩＣカード内で生成するシステムが提案されている（例えば、特許文献 1）。

【0003】

【特許文献 1】

特開 2 0 0 2 - 2 4 4 9 2 4 号公報

【0 0 0 4】

【発明が解決しようとする課題】

しかしながら、従来の I C カードは、デジタル署名用の秘密鍵を一つしか備えていなかった。そのため、特別なユーザに通常のユーザとは異なる秘密鍵を提供する場合、特別なユーザ用の秘密鍵を有する I C カードを製造し直さなければならず、特別なユーザ用の I C カードの製造コストが上昇してしまうという問題があった。

【0 0 0 5】

本発明は、このような問題に鑑みてなされたものであり、製造コストを高めることなく、特別なユーザに通常のユーザとは異なるデジタル署名用の鍵情報を提供できるようにすることを目的とする。

【0 0 0 6】

【課題を解決するための手段】

本発明におけるデジタル署名生成装置は、複数の秘密鍵を記憶した記憶手段とを有するデジタル署名生成装置であって、鍵変更コマンドを受信した場合には、前記デジタル署名生成装置が使用する秘密鍵を前記鍵変更コマンドが指定する秘密鍵に変更し、署名生成コマンドを受信した場合には、前記複数の秘密鍵の何れか一つを用いてデジタルデータのデジタル署名を生成することを特徴とする。

【0 0 0 7】

本発明におけるデジタル署名生成方法は、複数の秘密鍵を記憶した記憶手段とを有するデジタル署名生成装置におけるデジタル署名生成方法であって、鍵変更コマンドを受信した場合には、前記デジタル署名生成装置が使用する秘密鍵を前記鍵変更コマンドが指定する秘密鍵に変更する工程と、署名生成コマンドを受信した場合には、前記複数の秘密鍵の何れか一つを用いてデジタルデータのデジタル署名を生成する工程とを有することを特徴とする。

【0 0 0 8】

【発明の実施の形態】

以下、図面を参照し、本発明に好適な実施の形態を説明する。

## [第1の実施の形態]

まず、図1を参照し、第1の実施の形態におけるデジタル署名生成システムの主要な構成要素を説明する。

## 【0009】

ICカード10は、マルチアプリケーションOS (Operating System) を搭載したICカードであり、複数のアプリケーションプログラムの実行が可能なICカードである。ICカード10は、複数の秘密鍵を記憶した記憶媒体を有し、複数の秘密鍵の何れか一つを用いてデジタルデータM (画像データなど) のデジタル署名Sを生成することができる。ICカード10は、接触型であっても、非接触型であっても、ハイブリッド型 (接触型および非接触型の機能を有する) であってもよい。なお、ICカード10は、デジタルデータMのデジタル署名Sを生成する装置であるので、「デジタル署名生成装置」と呼ぶこともできる。

## 【0010】

コンピュータA20は、ベンダーが使用するコンピュータである。記録媒体A21は、コンピュータA20にインストールされるプログラムAを記録した記録媒体である。プログラムAは、コンピュータA20での実行が可能なプログラムであり、秘密鍵変更処理 (図5参照) および秘密鍵確認処理 (図6参照) の実行に必要なプログラムである。

## 【0011】

コンピュータB30は、通常又は特別なユーザが使用するコンピュータである。記録媒体B31は、コンピュータB30にインストールされるプログラムBを記録した記録媒体である。プログラムBは、コンピュータB30での実行が可能なプログラムであり、デジタル署名生成処理 (図7参照) の実行に必要なプログラムである。

## 【0012】

次に、図2を参照し、本実施の形態におけるICカード10の主要な構成要素を説明する。インターフェースユニット101は、コンピュータA20又はコンピュータB30から送信されたコマンドを受信し、受信したコマンドに対応するレスポンスをコンピュータA20又はコンピュータB30に送信するユニットで



ある。

#### 【 0 0 1 3 】

C P U (Central Processing Unit) 1 0 2 は、E E P R O M 1 0 4 が記憶する複数のアプリケーションプログラムに従って I C カード 1 0 の動作を制御するユニットである。

#### 【 0 0 1 4 】

R O M (Read Only Memory) 1 0 3 は、マルチアプリケーション O S、コマンドインタープリタを記憶するメモリである。マルチアプリケーション O S は、E E P R O M 1 0 4 が記憶する複数のアプリケーションプログラムを管理するオペレーティングシステムである。マルチアプリケーション O S には、入出力機能、暗号機能、ファイル管理機能、E E P R O M 1 0 4 に新しいアプリケーションプログラムを追加する機能、E E P R O M 1 0 4 が記憶するアプリケーションプログラムを削除する機能などがある。

#### 【 0 0 1 5 】

E E P R O M (Electrically Erasable and Programmable ROM) 1 0 4 は、複数の秘密鍵を管理する鍵管理テーブル、複数のアプリケーションプログラム、ユーザデータなどを記憶するメモリである。

#### 【 0 0 1 6 】

R A M (Random Access Memory) 1 0 5 は、C P U 1 0 2 およびコプロセッサ 1 0 6 が扱うデータを一時的に記憶するメモリである。

#### 【 0 0 1 7 】

コプロセッサ (Co-Processor) 1 0 6 は、E E P R O M 1 0 4 が記憶する複数の秘密鍵の一つを用いてデジタルデータ M のハッシュ値を暗号化することによってデジタルデータ M のデジタル署名 S を生成するユニットである。暗号化アルゴリズムには、R S A 暗号などの公開鍵暗号を利用する。

#### 【 0 0 1 8 】

次に、図 3 を参照し、I C カード 1 0 の E E P R O M 1 0 4 が記憶する鍵管理テーブルの一例を説明する。鍵管理テーブルは、I C カード 1 0 が使用する秘密鍵を管理する管理テーブルである。鍵管理テーブルには、図 3 に示すように、複

数個の秘密鍵（本実施の形態では16個）が登録されている。0番の秘密鍵は通常のユーザ用の秘密鍵である。製造直後のICカード10の秘密鍵は0番の秘密鍵に設定されている。1番～15番までの秘密鍵は特別なユーザ用の秘密鍵である。ある特別なユーザに3番の秘密鍵を提供する場合、ベンダーはコンピュータA20を使用してICカード10に鍵変更コマンド（3番の秘密鍵を指定）を送信する。鍵変更コマンドの実行が正常に終了すれば、ICカード10の秘密鍵は3番の秘密鍵となり、特別なユーザに通常のユーザとは異なる秘密鍵を提供することができる。

#### 【0019】

次に、図4を参照し、コンピュータA20又はコンピュータB30からICカード10に送信されるコマンドのデータフォーマット、および、ICカード10からコンピュータA20又はコンピュータB30に送信されるレスポンスのデータフォーマットを説明する。

#### 【0020】

コマンド識別コードフィールド401は、コマンドの種別を表すコマンド識別コードを格納するフィールドである。コマンドには、鍵変更コマンド、鍵確認コマンド、署名生成コマンドなどがある。鍵変更コマンドは、ICカード10が使用する秘密鍵をベンダーによって選択された秘密鍵に変更することをICカード10に要求するコマンドである。鍵確認コマンドは、ICカード10に設定されている秘密鍵の鍵番号をICカード10に問い合わせるコマンドである。署名生成コマンドは、ユーザによって選択されたデジタルデータMのデジタル署名Sを生成することをICカード10に要求するコマンドである。

#### 【0021】

コマンドデータ長フィールド402は、コマンドデータフィールド403のデータ長（バイト長）を格納するフィールドである。

#### 【0022】

コマンドデータフィールド403は、ICカード10に送信するデータを格納するフィールドである。鍵変更コマンドの場合、コマンドデータフィールド403にはICカード10に設定したい秘密鍵の鍵番号が格納される。鍵確認コマン

ドの場合、コマンドデータフィールド403には何も格納されない。署名生成コマンドの場合、コマンドデータフィールド403にはデジタルデータM（画像データなど）が格納される。

#### 【0023】

レスポンスデータ長フィールド404は、レスポンスデータフィールド405のデータ長（バイト長）を格納するフィールドである。

#### 【0024】

レスポンスデータフィールド405は、コマンドに対応するデータを格納するフィールドである。鍵変更コマンドの実行が正常に終了した場合、レスポンスデータフィールド405には鍵変更コマンドに従って設定された秘密鍵の鍵番号が格納される。鍵確認コマンドの実行が正常に終了した場合、レスポンスデータフィールド405にはICカード10に設定されている秘密鍵の鍵番号が格納される。署名生成コマンドの実行が正常に終了した場合、署名生成コマンドから取り出されたデジタルデータのデジタル署名が格納される。鍵変更コマンド、鍵確認コマンド又は署名生成コマンドの実行が正常に終了しなかった場合、レスポンスデータフィールド405にはダミーデータが格納される。

#### 【0025】

状態コードフィールド406は、コマンドを実行した結果（正常終了、エラー、警告など）を表す状態コードを格納するフィールドである。

#### 【0026】

次に、図5を参照し、コンピュータA20とICカード10との間で実行される秘密鍵変更処理の手順を説明する。秘密鍵変更処理は、ICカード10が使用する秘密鍵をベンダーが選択した秘密鍵に変更する処理である。秘密鍵変更処理は、ICカード10の製造後、ベンダー側で行われる処理である。

#### 【0027】

ステップS501：コンピュータA20は、ベンダーの指示に従って鍵変更コマンドを生成し、生成した鍵変更コマンドをICカード10に送信する。このとき、鍵変更コマンドのコマンドデータフィールド403には、ベンダーによって選択された鍵番号が格納されている。

## 【0028】

ステップS502：インターフェースユニット101は、鍵変更コマンドを受信し、受信した鍵変更コマンドをCPU102に供給する。CPU102は、鍵変更コマンドのコマンドデータフィールド403から鍵番号を取り出し、取り出した鍵番号を有効にするべく鍵管理テーブルを更新する。つまり、鍵変更コマンドが指定する秘密鍵をICカード10が使用する秘密鍵に変更する。例えば、鍵変更コマンドが指定する鍵番号が3番である場合、ICカード10が使用する秘密鍵は3番の秘密鍵に変更される。

## 【0029】

ステップS503：CPU102は、鍵変更コマンドを実行した結果からレスポンスを生成し、生成したレスポンスをインターフェースユニット101に供給する。このとき、レスポンスのレスポンスデータフィールド405には、変更後の鍵番号が格納されている。インターフェースユニット101は、レスポンスをコンピュータA20に返信する。

## 【0030】

ステップS504：コンピュータA20は、レスポンスを受信し、受信したレスポンスを解析する。鍵変更コマンドが正常に終了した場合、コンピュータA20は、変更後の鍵番号をベンダーに通知する。これにより、ベンダーは、ICカード10に設定されたデジタル署名用の秘密鍵を知ることができる。鍵変更コマンドが正常に終了しなかった場合、コンピュータA20は、状態コードを用いて鍵変更コマンドが正常に終了しなかった理由をベンダーに通知する。

## 【0031】

次に、図6を参照し、コンピュータA20とICカード10との間で実行される秘密鍵確認処理の手順を説明する。秘密鍵確認処理は、ICカード10が使用するデジタル署名用の秘密鍵を確認する処理である。秘密鍵確認処理は、ベンダー側で行われる処理である。

## 【0032】

ステップS601：コンピュータA20は、ベンダーの指示に従って鍵確認コマンドを生成し、生成した鍵確認コマンドをICカード10に送信する。このと

き、鍵確認コマンドのコマンドデータフィールド403には、何も格納されていない。

#### 【0033】

ステップS602：インターフェースユニット101は、鍵確認コマンドを受信し、受信した鍵確認コマンドをCPU102に供給する。CPU102は、インターフェースユニット101から供給された鍵確認コマンドを実行する。CPU102は、鍵管理テーブルを参照し、ICカード10に設定されている鍵番号を調べる。

#### 【0034】

ステップS603：CPU102は、鍵確認コマンドを実行した結果からレスポンスを生成し、生成したレスポンスをインターフェースユニット101に供給する。このとき、レスポンスのレスポンスデータフィールド405には、ICカード10に設定されている鍵番号が格納されている。インターフェースユニット101は、レスポンスをコンピュータA20に返信する。

#### 【0035】

ステップS604：コンピュータA20は、レスポンスを受信し、受信したレスポンスを解析する。鍵確認コマンドが正常に終了した場合、コンピュータA20は、ICカード10に設定されている鍵番号をベンダーに通知する。これにより、ベンダーは、ICカード10に設定されているデジタル署名用の秘密鍵を知ることができる。鍵確認コマンドが正常に終了しなかった場合、コンピュータA20は、状態コードを用いて鍵確認コマンドが正常に終了しなかった理由をベンダーに通知する。

#### 【0036】

次に、図7を参照し、コンピュータB30とICカード10との間で実行されるデジタル署名生成処理の手順を説明する。デジタル署名生成処理は、ICカード10に設定されているデジタル署名用の秘密鍵を用いてデジタルデータMのデジタル署名Sを生成する処理である。デジタル署名生成処理は、通常又は特別なユーザ側で行われる処理である。

#### 【0037】

ステップS701: コンピュータB30は、通常又は特別なユーザの指示に従って署名生成コマンドを生成し、生成した署名生成コマンドをICカード10に送信する。このとき、署名生成コマンドのコマンドデータフィールド403には、デジタルデータMが格納されている。

#### 【0038】

ステップS702: インターフェースユニット101は、署名生成コマンドを受信し、受信した署名生成コマンドをCPU102に供給する。CPU102は、鍵変更コマンドのコマンドデータフィールド403からデジタルデータMを取り出し、取り出したデジタルデータMをRAM105に書き込む。CPU102は、鍵管理テーブルからICカード10に設定されている秘密鍵を取り出し、取り出した秘密鍵をRAM105に書き込む。コンピュータB30のユーザが通常のユーザである場合、CPU102は、0番の秘密鍵をRAM105に書き込む。コンピュータB30のユーザが特別なユーザである場合、コプロセッサ106は、1番から15番の何れかの秘密鍵をRAM105に書き込む。コプロセッサ106は、デジタルデータMのデジタル署名Sを生成するために、RAM105から読み出したデジタルデータMからデジタルデータMのハッシュ値を生成し、生成したハッシュ値をRAM105から読み出した秘密鍵によって暗号化する。コプロセッサ106は、生成したデジタル署名SをRAM105に書き込む。

#### 【0039】

ステップS703: CPU102は、署名生成コマンドを実行した結果からレスポンスを生成し、生成したレスポンスをインターフェースユニット101に供給する。署名生成コマンドの実行が正常に終了した場合、レスポンスデータフィールド405にはRAM105から読み出されたデジタル署名Sが格納される。署名生成コマンドの実行が正常に終了しなかった場合、レスポンスデータフィールド405にはダミーデータが格納される。インターフェースユニット101は、レスポンスをコンピュータB30に返信する。

#### 【0040】

ステップS704: コンピュータB30は、レスポンスを受信し、受信したレスポンスを解析する。署名生成コマンドの実行が正常に終了した場合、コンピュ

ータ B 3 0 は、デジタル署名 S が正常に生成されたことをユーザに通知する。そして、コンピュータ B 3 0 は、レスポンスデータフィールド 4 0 5 からデジタル署名 S を取り出し、取り出したデジタル署名 S をデジタルデータ M に付加する。署名生成コマンドの実行が正常に終了しなかった場合、コンピュータ B 3 0 は、正常に終了しなかった理由をユーザに通知する。

#### 【 0 0 4 1 】

次に、図 8 を参照し、特別なユーザ用の秘密鍵を設定した I C カード 1 0 を特別なユーザに提供する手順を説明する。

#### 【 0 0 4 2 】

ステップ S 8 0 1 : ベンダーは、特別なユーザから I C カード 1 0 を受け取る。

#### 【 0 0 4 3 】

ステップ S 8 0 2 : ベンダーは、特別なユーザに使用させる鍵番号（1 番から 1 5 番までの何れか）を決定する。

#### 【 0 0 4 4 】

ステップ S 8 0 3 : ベンダーは、ステップ S 8 0 2 で決定した鍵番号を I C カード 1 0 に設定する。鍵番号の設定には、上記の鍵変更コマンドを使用する。この処理により、I C カード 1 0 には通常のユーザとは異なる秘密鍵が設定される（通常のユーザの鍵番号は 0 番である）。例えば、ステップ S 8 0 2 で決定した鍵番号が 3 番である場合、I C カード 1 0 の秘密鍵は 3 番に対応する秘密鍵となる。

#### 【 0 0 4 5 】

ステップ S 8 0 4 : ベンダーは、I C カード 1 0 を特別なユーザに提供する。これにより、ベンダーは、特別なユーザに通常のユーザとは異なるデジタル署名用の秘密鍵を提供することができる。

#### 【 0 0 4 6 】

このように、第 1 の実施の形態における I C カード 1 0 によれば、鍵変更コマンドによって使用する秘密鍵を変更することができるので、I C カード 1 0 の製造コストを高めることなく、特別のユーザに通常のユーザとは異なるデジタル署

名用の秘密鍵を提供することができる。また、特別なユーザ用の秘密鍵を複数個記憶することもできるので、特別なユーザが複数存在する場合であっても、それぞれに通常のユーザとは異なるデジタル署名用の秘密鍵を提供することもできる。

#### 【0047】

また、第1の実施の形態におけるICカード10によれば、マルチファンクションOSを搭載しているので、新しいアプリケーションプログラムの追加を容易にすることができる。つまり、デジタル署名の生成アルゴリズムを新しくすることも、上記の鍵管理テーブルを更新することも、全く新しい機能を追加することも容易にできるようになる。

#### 【0048】

##### [第2の実施の形態]

上記のデジタル署名生成処理では、署名生成コマンドのコマンドデータフィールドにデジタルデータMを格納したが、デジタルデータMをデジタルデータMのハッシュ値に置き換えることも可能である。この場合、ICカード10内でデジタルデータMのハッシュ値を生成しなくてもよくなるため、ICカード10にかかる負荷を軽減することができ、デジタル署名Sを高速に生成することができるようになる。またこの場合、ICカード10で扱うデータサイズを小さくすることができるので（なぜなら、デジタルデータMのハッシュ値のデータサイズはデジタルデータMのデータサイズよりも十分に小さいため）、ICカード10の回路規模を小さくでき、ICカード10の製造コストをより安くすることができる。

#### 【0049】

##### [第3の実施の形態]

上記のコンピュータB30は、デジタルカメラ、デジタルビデオカメラ、スキャナなどの撮像装置に置き換えることも可能である。第2の実施の形態におけるデジタル署名生成システムの主要な構成要素を図9に示す。撮像装置40は、被写体の画像データを撮像する撮像ユニットを有する装置であり、例えば、デジタルカメラ、デジタルビデオカメラ、スキャナである。記録媒体41は、上記のデ



デジタル署名生成処理の実行に必要なプログラムを記録した記録媒体である。この場合、撮像装置 4 0 で撮像されたオリジナル画像データのデジタル署名を I C カード 1 0 で生成することが可能になる。

#### 【 0 0 5 0 】

##### [その他の実施の形態]

上述した実施の形態の機能を実現するべく各種のデバイスを動作させるように、該各種デバイスと接続された装置或いはシステム内のコンピュータに対し、上記実施の形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステム或いは装置のコンピュータ（C P U 或いは M P U）に格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

#### 【 0 0 5 1 】

また、この場合、上記ソフトウェアのプログラムコード自体が上述した実施の形態の機能を実現することになり、そのプログラムコード自体は本発明を構成する。そのプログラムコードの伝送媒体としては、プログラム情報を搬送波として伝搬させて供給するためのコンピュータネットワーク（L A N、インターネット等の W A N、無線通信ネットワーク等）システムにおける通信媒体（光ファイバ等の有線回線や無線回線等）を用いることができる。

#### 【 0 0 5 2 】

さらに、上記プログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記憶する記録媒体としては、例えばフレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、C D - R O M、磁気テープ、不揮発性のメモ리카ード、R O M等を用いることができる。

#### 【 0 0 5 3 】

また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施の形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働している O S（オペレーティングシステム）或いは他のアプリケーションソフト等と共同して上述の実施の形態の機能が実現される場合にも

かかるプログラムコードは本発明の実施の形態に含まれることはいうまでもない。

#### 【0 0 5 4】

さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるCPU等が実際の処理の一部又は全部を行い、その処理によって上述した実施の形態の機能が実現される場合にも本発明に含まれることはいうまでもない。

#### 【0 0 5 5】

なお、上記実施の形態において示した各部の形状および構造は、何れも本発明を実施するにあたっての具体化のほんの一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、又はその主要な特徴から逸脱することなく、様々な形で実施することができる。

#### 【0 0 5 6】

##### 【発明の効果】

以上説明したように本発明によれば、製造コストを高めることなく、特別なユーザに通常のユーザとは異なるデジタル署名用の秘密鍵を提供することができる。

##### 【図面の簡単な説明】

##### 【図 1】

第 1 の実施の形態におけるデジタル署名生成システムの主要な構成要素を示す図である。

##### 【図 2】

ICカード 1 0 の主要な構成要素を示す図である。

##### 【図 3】

鍵管理テーブルの一例を示す図である。

##### 【図 4】

コマンドおよびレスポンスのデータフォーマットを示す図である。

**【図 5】**

秘密鍵変更処理の手順を説明する図である。

**【図 6】**

秘密鍵変更処理の手順を説明する図である。

**【図 7】**

デジタル署名生成処理の手順を説明する図である。

**【図 8】**

特別なユーザ用の秘密鍵を設定した I C カード 1 0 を特別なユーザに提供する手順を説明する図である。

**【図 9】**

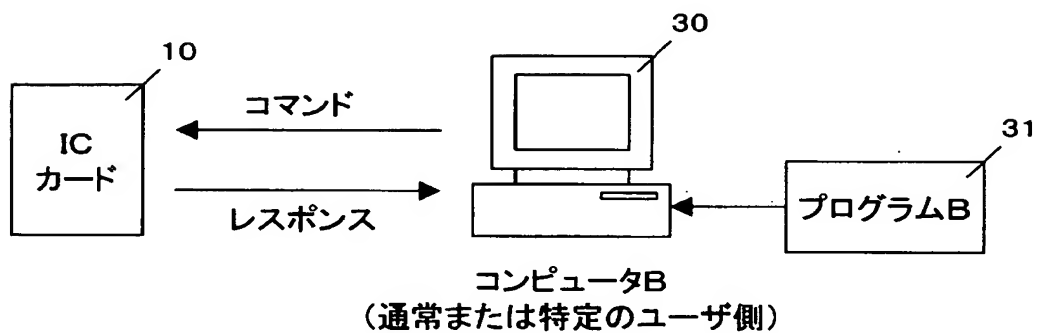
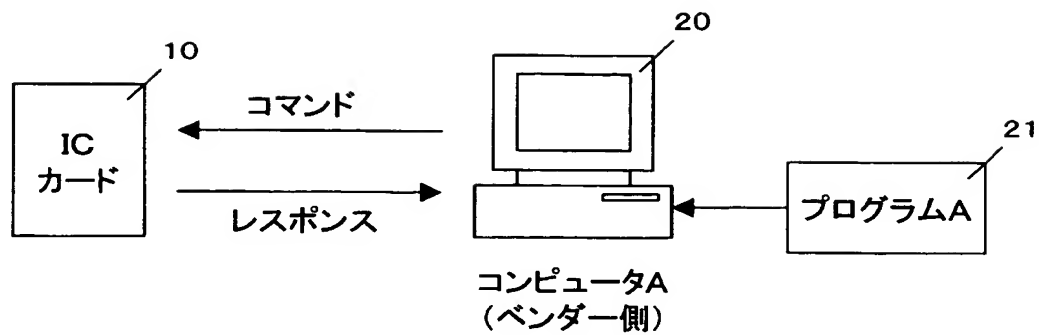
第 3 の実施の形態におけるデジタル署名生成システムの主要な構成要素を示す図である。

**【符号の説明】**

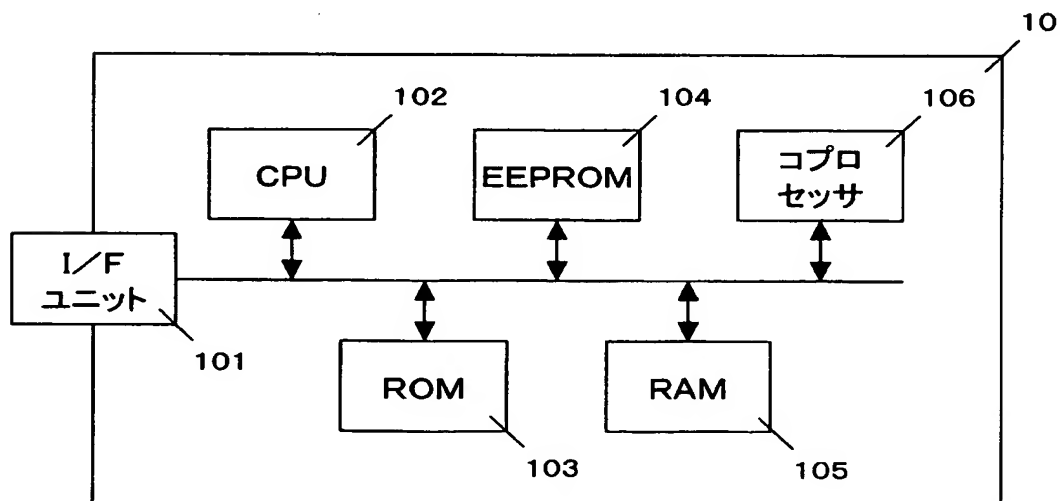
- 1 0    I C カード
- 2 0    コンピュータ A
- 2 1    記録媒体 A
- 3 0    コンピュータ B
- 3 1    記録媒体 B
- 1 0 1   インターフェースユニット
- 1 0 2   C P U
- 1 0 3   R O M
- 1 0 4   E E P R O M
- 1 0 5   R A M
- 1 0 6   コプロセッサ

【書類名】 図面

【図 1】



【図 2】



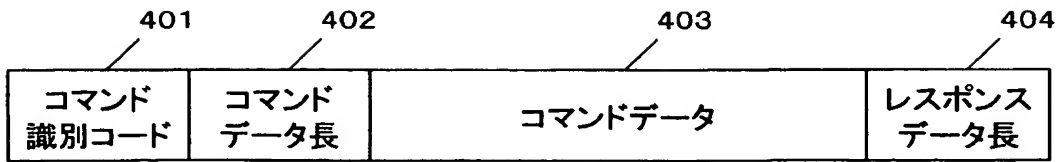
【図 3】

フラグ	鍵番号	秘密鍵	
ON	0	0x9876543210AB...	通常のユーザ用の秘密鍵
OFF	1	0x876543210ABC...	
OFF	2	0x76543210ABCD...	特定のユーザ用の秘密鍵
:	:	:	
OFF	15	0xF9876543210A...	

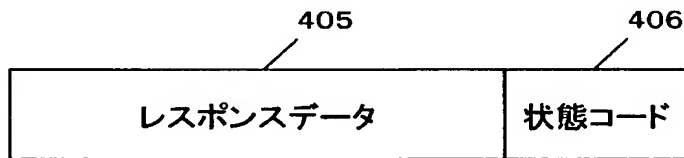
鍵設定コマンド(鍵番号3を指定)を実行した後

フラグ	鍵番号	秘密鍵	
OFF	0	0x9876543210AB...	通常のユーザ用の秘密鍵
OFF	2	0x876543210ABC...	
ON	3	0x76543210ABCD...	特定のユーザ用の秘密鍵
:	:	:	
OFF	15	0xF9876543210A...	

【図 4】

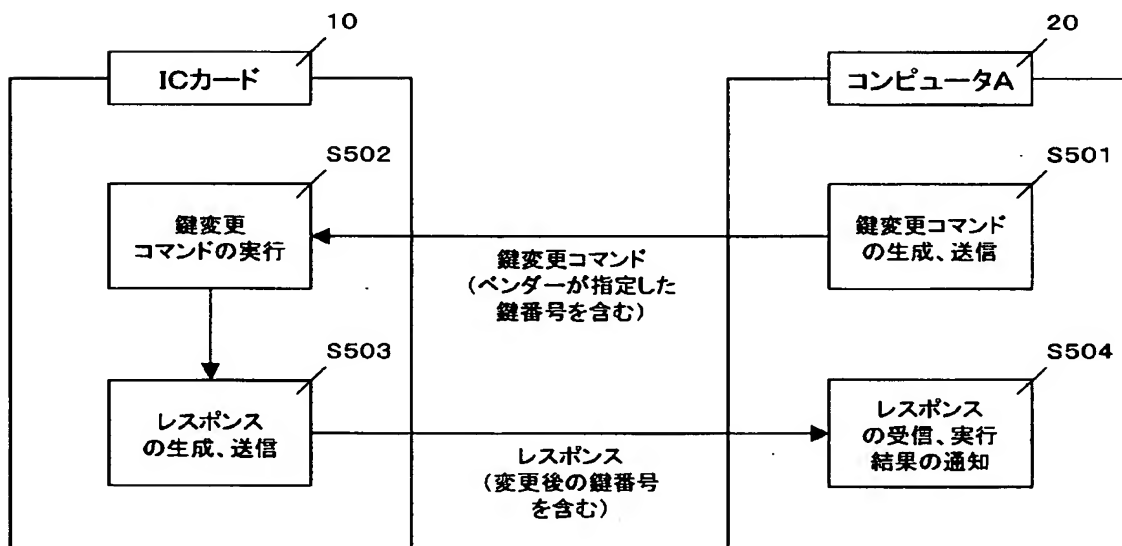


(a)コマンドのデータフォーマット

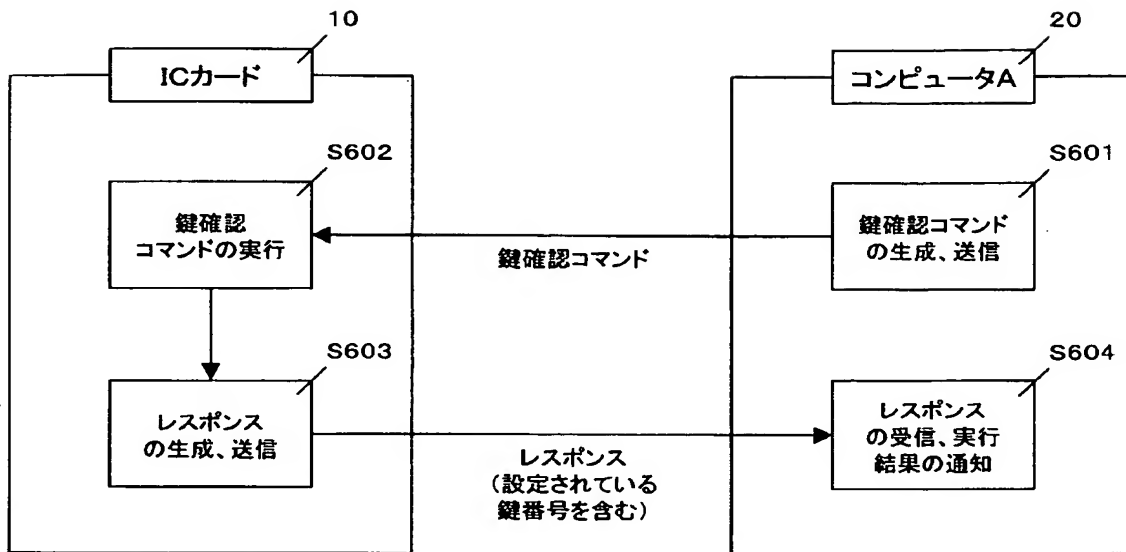


(b)レスポンスのデータフォーマット

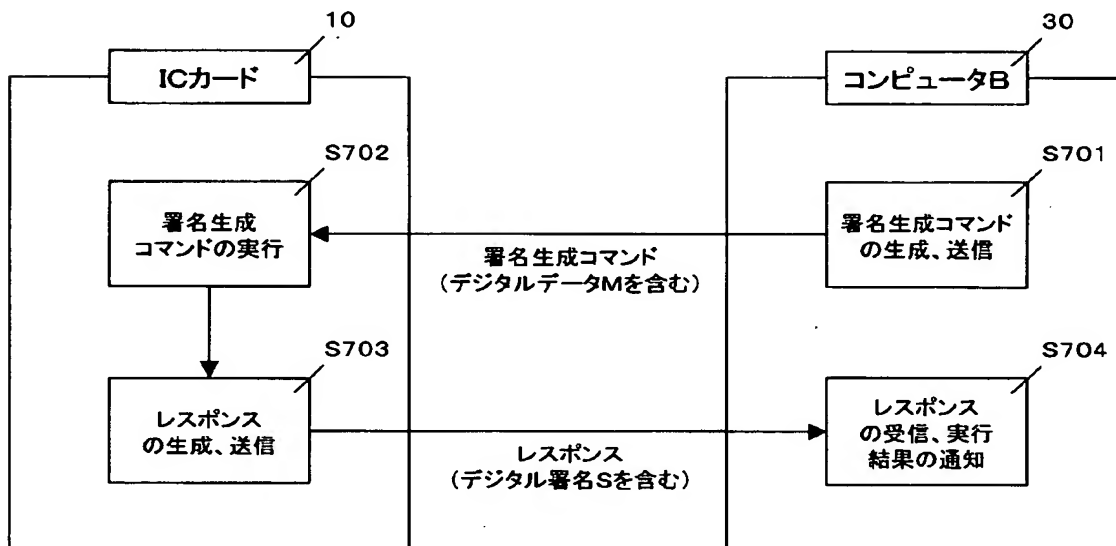
【図 5】



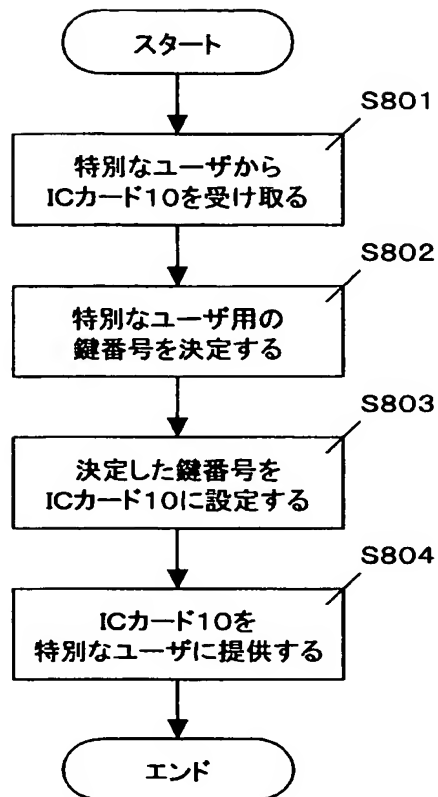
【図 6】



【図 7】

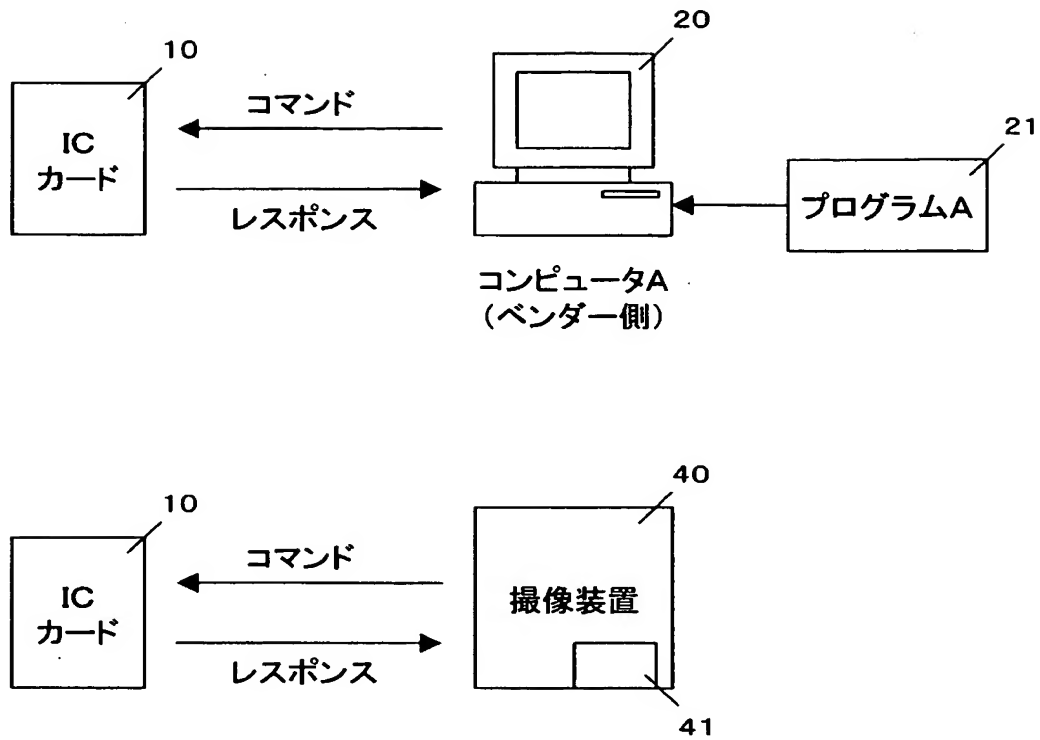


【図 8】





【図 9】



【書類名】 要約書

【要約】

【課題】 製造コストを高めることなく、特別なユーザに通常のユーザとは異なるデジタル署名用の秘密鍵を提供できるようにする。

【解決手段】 複数のデジタル署名用の秘密鍵を記憶する E E P R O M 1 0 4 と、複数の秘密鍵の何れか一つを用いてデジタルデータのデジタル署名を生成するコプロセッサ 1 0 6 とを有し、鍵変更コマンドを受信した場合には、 I C カード 1 0 が使用する秘密鍵を鍵変更コマンドが指定する秘密鍵に変更する I C カード 1 0 を提供する。

【選択図】 図 2

特願 2 0 0 3 - 0 7 1 0 3 3

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 1 0 0 7 ]

1. 変更年月日 1 9 9 0 年 8 月 3 0 日

[変更理由] 新規登録

住 所 東京都大田区下丸子 3 丁目 3 0 番 2 号

氏 名 キヤノン株式会社